PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-304809
(43)Date of publication of application : 18.10.2002

(51)Int.Cl. G11B 20/10
G06F 12/14
G11B 7/004
G11B 7/26
G11B 20/12

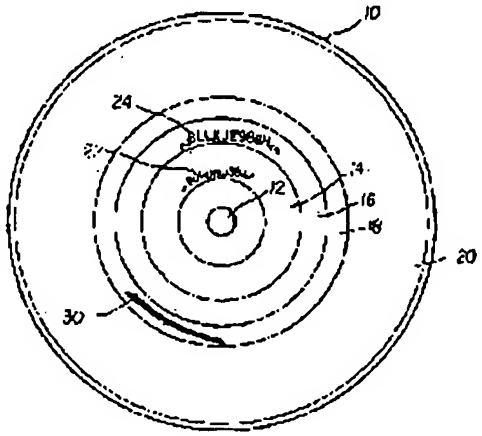
(21)Application number : 2002-018468
(22)Date of filing : 28.01.2002

(71)Applicant : EASTMAN KODAK CO
(72)Inventor : BARNARD JAMES A
INCHALIK MICHAEL A
HA BRUCE L

(30)Priority
Priority number : 2001 772333 Priority date : 29.01.2001 Priority country : US

(54) COPY PROTECTION USING A PREFORMED ID AND A UNIQUE ID ON A PROGRAMMABLE CD-ROM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for making copy protection that cannot be subverted by a bit-for-bit copying scheme on standard CD-writers.
SOLUTION: This invention provides a copy-protected optical disk, including a pre-formed ID, which is impressed upon the optical disk during optical disk manufacture, a unique ID which was written on the optical disk after it is manufactured, and an encrypted program written onto the optical disk wherein the encryption of such program is based upon the performed ID and the unique ID.



LEGAL STATUS

[Date of request for examination]	24.01.2005
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	withdrawal
[Date of final disposal for application]	27.04.2005

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－304809
（P2002－304809A）
(43)公開日　平成14年10月18日(2002.10.18)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０１７
	３０１		３０１Ｚ	５Ｄ０４４
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｄ０９０
Ｇ１１Ｂ　7/004		Ｇ１１Ｂ　7/004	Ｚ	５Ｄ１２１
7/26		7/26		

審査請求　未請求　請求項の数３　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2002－18468(P2002－18468)

(22)出願日　平成14年１月28日(2002.1.28)

(31)優先権主張番号　７７２３３３

(32)優先日　平成13年１月29日(2001.1.29)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000846
イーストマン　コダック　カンパニー
アメリカ合衆国，ニューヨーク14650，ロチェスター，ステイト　ストリート343

(72)発明者　ジェイムズ　エイ　バーナード
アメリカ合衆国　ニューヨーク　14546
スコッツヴィル　チリ・アヴェニュー　51

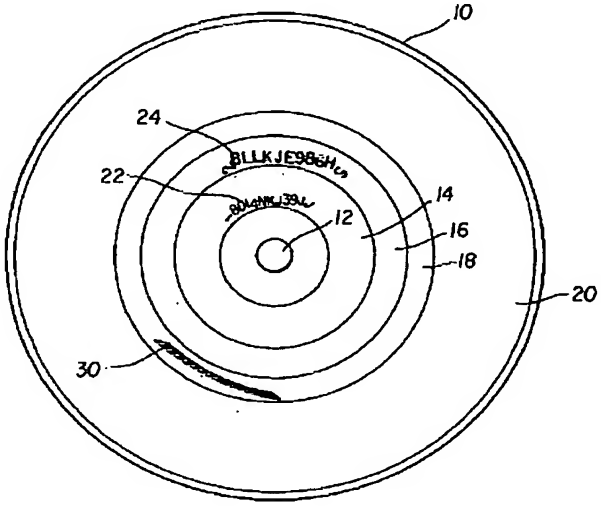
(72)発明者　マイケル　エイ　インチャリック
アメリカ合衆国　ニューヨーク　14534
ピッツフォード　カッパー・ウッズ　30

(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　予め形成されたＩＤおよび固有のＩＤを利用したプログラム可能なＣＤ－ＲＯＭにおけるコピー・プロテクト

(57)【要約】
【課題】　標準的なＣＤライタでビットに関するコピー手法によって破られないコピー・プロテクトを行う手法を提供すること。
【解決手段】　本発明によれば、コピー・プロテクトされた光学ディスクが提供される。光学ディスクは、光学ディスクの製造中に光学ディスクに記された予め形成されたＩＤと、製造後に前記光学ディスクに書き込まれた固有のＩＤと、光学ディスク上に書き込まれた暗号化されたプログラムとを有する。そのプログラムの暗号化は、前記予め形成されたＩＤおよび前記固有のＩＤに基づいて行われる。



【特許請求の範囲】
【請求項１】　コピー・プロテクトされた光学ディスクであって：
ａ）光学ディスクの製造中に光学ディスクに記された予め形成されたＩＤ；
ｂ）製造後に前記光学ディスクに書き込まれた固有のＩＤ；および
ｃ）前記光学ディスク上に書き込まれた暗号化されたプログラム；
より成り、そのプログラムの暗号化は、前記予め形成されたＩＤおよび前記固有のＩＤに基づいて行われることを特徴とする光学ディスク。
【請求項２】　光学ディスクに記録された情報をコピー・プロテクトする方法であって：
ａ）予め形成されたＩＤを含むマスタ・ディスクを形成するステップ；
ｂ）前記マスタ・ディスクと同一の予め形成されたＩＤを有する複数の光学ディスクを形成するステップ；
ｃ）光学ディスクに固有の識別番号を書き込むステップ；および
ｄ）前記光学ディスクに暗号化されたプログラムを書き込むステップ；
より成り、そのプログラムの暗号化は、前記予め形成されたＩＤおよび前記固有のＩＤに基づいて行われることを特徴とする方法。
【請求項３】　プログラム可能なＣＤ－ＲＯＭおよび暗号化解除プログラムを利用してコピー・プロテクトを行う方法であって：
ａ）プログラム可能なＣＤ－ＲＯＭの予め形成されたＩＤおよび固有のＩＤを読み出すステップ；
ｂ）前記予め形成されたＩＤおよび固有のＩＤを結合して暗号解除キーを作成するステップ；
ｃ）前記暗号解除キーを利用して、当初の実行可能なファイルの暗号化を解除するステップ；
ｄ）当初の実行可能なものをコンピュータのＲＡＭメモリに格納し、それを実行することを許容するステップ；および
ｅ）前記実行可能なものの実行完了時に、前記コンピュータのメモリから前記当初の実行可能なものを削除するステップ；
より成ることを特徴とする方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンパクト・ディスクその他の光学的に記録されたディスクに記録された情報に対するコピー・プロテクトに関する。
【０００２】
【従来の技術】オーディオ、映像、ソフトウエアまたはデータを含む光学ディスクの消費者購買層は数十億ドル市場を生み出した。近年おける低価格の光学的記録媒体およびドライバの出現は、権限なしにその内容をコピーすることを普及させた。これに対処するために、様々なコピー・プロテクト手法が開発された。しかしながらこれらの手法の内のあるものは、ディジタル・データ・ストリームの特徴を利用し、これは精巧な低価格のレコーダにより、ビットに関するコピー(bit-for-bit copy)を利用してコピーされ得る。他には、書き込みおよび読み込みの両者を困難にするように光学ディスクの特徴を変化させるものがある。さらには、ネットワーク接続または２次的な「キー」(key)ディスク手法を使用し、独立した（スタンドアロンの）プロテクトを許容しないものもある。
【０００３】Horstmann(U.S. 6,044,469)は、プロテクタ・モジュールを利用したソフトウエア保護機構を開示し、これはライセンス・ファイルを読み出し、購入したそのライセンスに基づく規則を実行する。これは論理レベルにおけるソフトウエアを保護し、特に、権利が認められていないソフトウエアの部分に対する保護である。このシステムがコンパクト・ディスクに包含されるならば、標準的なＣＤライタを利用したそのディスクの再生成は、総ての既存のアクセスに関するコピーを正当なものにするであろう。
【０００４】Asai et al(U.S.Re. 35,839)は、データを格納するコンパクト・ディスクにおける識別領域を利用する方法を開示し、これはディスクの他の場所に格納されたデータと比較され、真正であることを確認する。これは論理レベルにおけるデータを保護するが、そのディスクに関する単純なビットに関するコピーによって、そのプロテクトは破られてしまう。
【０００５】DeMont(U.S. 5,982,889)は、情報製品(information product)に対するユーザ・アクセスが真正であることを確認する方法を教示する。このシステムの欠点は、その真正確認が中央局を介して行われることである。ネットワークに接続することを希望しない（または不可能な）ユーザは、この製品を利用することができない。
【０００６】Hasebe, et al(U.S. 5,555,304)は、ユーザ各自または使用されるコンピュータに関連するシステムを開示する。これは、単独のコンピュータにおけるプログラムの利用を真正のユーザに限定し、ユーザの移動性またはそれらの設備のアップ・グレードを非常に制限する。さらに、この特許は、ディスクの再書き込み不可能な領域に格納されたデータの利用にも関連し、再書き込み不可能なリーフ(leaves)が形成されるその手法は、（「再書き込み不可能な」部分も含めて）データを新たなディスクにコピーする機能を開放する。
【０００７】Fite et alによる一連の特許(U.S. 5,400,319, 5,513,169, 5,541,904, 5,805,549, および5,930,215)は、規定可能なコードを生成するようにディスクの小領域から反射層を選択的に除去することによって、光

学ディスクに機械的に読み取り可能なシリアル番号コードを形成する方法を開示する。このようなシステムに対する欠点は、この特殊なコードを書き込むために特殊な装置が必要とされることである。

【０００８】Kanamaru(U.S. 5,940,505)は、どのようにしてＣＤ－ＲＯＭがコピー・プロテクトされるかを教示する。しかしながら、Kanamaru の発明の総ての装置は、ディスク上の情報を解読するために、組み込み回路形式でまたは付加的なコンピュータ・ボード形式で、補助的なハードウエアを要する。

【０００９】O' Connor et al.による米国特許第5,745,568号は、特定のコンピュータ・システムによって回復されるＣＤ－ＲＯＭデータを保全する方法およびシステムを開示する。光学ディスクの領域は、暗号キーとしてのハードウエア識別子を用いて暗号化される。ハードウエア識別子は、選択されたコンピュータ・ハードウエアに関連する。ＣＤ－ＲＯＭに含まれるソフトウエア・プログラム・ファイルは、暗号キーとしてのハードウエア識別子を利用して暗号化される。ＣＤ－ＲＯＭ上の選択されたソフトウエア・プログラムは、暗号キーとしてのハードウエア識別子を利用するソフトウエア・プログラム・ファイルを解読することによって、その選択されたコンピュータ上でインストールされる。

【００１０】Akiyama et al.による米国特許第5,805,699号は、マスタ記憶媒体に記録された著作物ソフトウエアを、合法的な手法で、ユーザのターゲット記憶媒体にコピーさせることを可能にするソフトウエア・コピー・システムを提案する。マスタ記憶媒体（すなわち、ＣＤ－ＲＯＭ）は、ソフトウエア識別子を有し、ターゲット記憶媒体は記憶媒体識別子を有する。これら２つの識別子が中央局に伝送され、中央局はソフトウエア製品をコピーするための権利に関するライセンス（契約）を管理している。中央局において、２つの識別子から第１の署名が生成され、コンピュータ・ユーザに返送される。ユーザのコンピュータにおいて、その２つの識別子から第２の署名が生成される。２つの署名が互いに一致する場合に限って、マスタ記憶媒体からターゲット記憶媒体へソフトウエア・プログラムがコピーされ得る。

【００１１】Chandra et al.による米国特許第4,644,493号は、単独のコンピュータで使用する磁気媒体で使用されるソフトエアの拡布を制限する方法および装置を開示する。磁気媒体に含まれる当初のソフトウエアは、機能的にコピー不可能である。これは、コンピュータの一部をなす不正操作のきかないコプロセッサに格納されたプログラムを実行することによってそれが修正されるまでその状態が続く。

【００１２】Indeck et al.による米国特許第5,740,244号は、磁気媒体上のソフトウエア製品が最初にコンピュータに命令することによる改善を開示し、その磁気媒体を挿入すると、その製品の特定の部分の指紋を読み取り、その指紋とその同じ指紋に関して予め記録されていたものとを比較する。指紋が一致していれば、ソフトウエア製品は、コンピュータが更に読み込むことを許容し、そこに格納されているアプリケーション・ソフトウエアを実行可能にする。

【００１３】これらの手法に関連して多くの問題が存在する。１つには、これらの多くが「ハック」(hacks)と呼ばれるものに対して無防備なことである。これの意味することは、あるユーザが解読する又はそのアプリケーションを利用する方法を判別すると、その種の者にとって、そのアプリケーションへのアクセスを取得する方法を広めることは非常に容易であるということである。特定のハードウエアの組み合わせに依存した特定のアプリケーションを利用することによって、この問題を解決するものもある。その手法は携帯性に関する問題を生み出す。合法的なユーザであっても場所が異なればコンピュータ上のアプリケーションを利用できないのである。ユーザが、例えばアップ・グレードによりハードウエアの構成(configuration)を変更すると、そのアプリケーションは起動することができない。

【００１４】

【発明が解決しようとする課題】従って、本発明は、標準的なＣＤライタでビットに関するコピー手法によって破られないコピー・プロテクトを行う手法を提供することを目的とする（ただし、これは標準的なＣＤマスタおよびライト設備で実行可能なものである。）。

【００１５】

【課題を解決するための手段】この課題を解決するコピー・プロテクトされた光学ディスクは：

ａ）光学ディスクの製造中に光学ディスクに記された予め形成されたＩＤ；

ｂ）製造後に前記光学ディスクに書き込まれた固有のＩＤ；および

ｃ）前記光学ディスク上に書き込まれた暗号化されたプログラム；

より成り、そのプログラムの暗号化は、前記予め形成されたＩＤおよび固有の識別番号に基づいて行われる光学ディスクである。

【００１６】本発明は、一般のハッカによる発見を防止しつつ携帯性をも提供し、認証されているユーザが単独のコンピュータ・システムを利用することに関して制限されないようにする。多くの従来技術とは異なり、ソフトウエアが利用される又はインストールされるときに、接触する権限を付与する中央管理的な権利は必要としない。

【００１７】物理的形態のキー（予め形成されたＩＤ）および論理的形態のキー（固有のＩＤ）の両者を利用することによって、多くの複製手法を排除する。単純なビットに関する複製(bit-for-bit duplication)が回避される。なぜなら、予め形成されたＩＤをコピーしないか

らであり、これはディスク・トラックの物理的構造に符号化されている。複数ユーザまたは複数の顧客の間でのソフトウエアの「共有」が回避される。なぜなら、そのように共有されるソフトウエアは、（よく起こるであろう事態として）両ユーザが予め形成されたＩＤを利用してディスクを使用しようとする場合であっても、適切な固有のＩＤなしには走らないからである。その記録手法は、ロック(lock)された実行可能なファイルを形成する。

【００１８】

【発明の実施の形態】図１を参照するに、本発明によるコピー・プロテクトされた光学ディスク１０が示されている。これはプログラム可能なＣＤ－ＲＯＭディスクであり、予め記録されたマスタ領域(mastered pre-recorded area)（ＲＯＭ領域）および記録可能な領域（ＲＡＭ領域）の両者を含む。ディスク１０を回転指させるための中心軸に関するホール１２がある。この特定のプログラム可能なＣＤ－ＲＯＭディスクは、マスタ化された第１セッション(session)１４を有し；すなわち、マスタ・ディスクが、第１セッション１４において供給されるソフトウエアまたはデータを包含して形成され、その後に、直接的に又は中間的な「父」および「母」ディスクを介して、ディスク１０の多くのコピーに印を付すために使用される。プログラム可能なＣＤ－ＲＯＭをマスタ化する技術は、本願と共通して譲渡され、２０００年９月１５日付けで出願され、Ha et alによる “System for Making aPhotoresist Master of a Hybrid Optical Recording Disc” と題する米国特許出願番号09／662,561号に詳細に説明されており、その開示内容は本願でも使用可能である。

【００１９】プログラム可能なＣＤ－ＲＯＭを含む書き込み可能なコンパクト・ディスクは、部分的に溝変調(groove modulation)を使用する。ディスク１０は、基板の内側端部から外側端部に伸びる連続的ならせん状トラックを有する。らせん状トラックは通常は溝であり、ディスク１０にデータ・チャネルを提供し、データの読み込みまたは書き込みの最中にディスク１０のトラッキング(tracking)をも提供する。溝はその溝に垂直な方向の振動を有し、それゆえに揺動した溝(wobbled groove)または逓動的な溝(wobble groove)としても言及される。データをアドレスおよびプログラムする配置に加えて、プログラム可能なＣＤ－ＲＯＭ光学記録ディスクのトラック又は溝，溝の変調度は、オレンジ・ブック・パート２仕様1(Orange Book Part II specification)に従って提供されるのが普通である。「オレンジ・ブック・パート２」は、フィリップス・インターナショナルＢＶにより公表された仕様であり、記録可能なコンパクト・ディスク媒体のキー(key)特性および記録特性を規定する。

【００２０】溝の振動周波数は、プレ・グルーブにおける絶対時間(ATIP: Absolute Time In Pre-groove)として知られる信号を利用して変調される。ＡＴＩＰは、光学ディスク１０の記録面全体に関するトラックの場所に関する情報を含む。オレンジ・ブック仕様によれば、ＡＴＩＰ信号は２２．０５ｋＨｚのＦＭ信号であり、３１５０ビット／秒のレートでデータを搬送する。このデータは、毎秒７５４２ビット・フレームとして特定される。データ領域において、各フレームは、４つの同期ビットと、分カウントを表現する８ビットと、秒カウントを表現する８ビットと、フレーム・カウントを表現する８ビットより成る。分、秒およびフレーム・カウントは、２つの４ビット２進化１０進数（ＢＣＤ）より成る。ディスク１０のデータ領域において、これらの値の任意のものについての最大値は７５であり、各々の最上位ビット（ＭＳＢ）は常にゼロである。そして、分カウント、秒カウントおよびフレーム・カウントの最上位ビットの３つは、全体として、０００の２進値を有する。各フレームの最後の１４ビットは、巡回冗長検査(CRC: cyclic redundancy check)誤り保護として提供される。

【００２１】直径４６ｍｍないし５０ｍｍの間のディスク１０の領域として定義されるディスク導入領域(lead-in area)において、ＭＳＢの値は０００から変化する。１００という値は、そのフレームが、電力校正領域(Power Calibration Area)、プログラム・メモリ領域または導入領域(Lead-In Area)に関する時間コードを含むことを意味し、これら総てはプログラム（記録可能な）領域の前に設けられる。他のＭＳＢ値は、ＡＴＩＰフレームが特殊な制御コードを含むことを規定するために使用される。これらのコードは、例えば、ディスク１０に関する最適な書き込み電力、参照速度、ディスク・アプリケーション・コード、ディスク形式および副形式、導入領域の開始位置またはディスク１０に関する導出領域(Lead-Out Area)の開始位置を指示するために使用される。

【００２２】プログラム可能なＣＤ－ＲＯＭ光学ディスクのＲＯＭ領域において、溝は、データをアドレスするディスク１０およびデータをプログラムするディスクに対応してくぼんだ形状で(depression)更に変調される。ＣＤ上でオーディオでない情報が格納されているフォーマットは、「イエロー・ブック」(Yellow Book)規格として知られている。

【００２３】ディスク１０の第１セッション１４（ＲＯＭ領域）は、予め形成された識別番号またはＩＤ２２を含み、これはマスタ・プロセスの間に記録され、そして各プログラム可能なＣＤ－ＲＯＭディスクに押印されたディジタル署名である。予め形成されたＩＤ２２は、ＡＴＩＰ信号内にまたはディスク・プログラム可能なＣＤ－ＲＯＭ・データ信号内に設けることが可能である。好適実施例では、１つ又はそれ以上の特定の制御コードを利用して、導入領域におけるＡＴＩＰ信号に設けられる。例えば、ディスク・アプリケーション・コード、ディスク形式、ディスクに関する最適な書き込み電力、参

照速度、導入領域の開始位置、導出領域の開始位置、またはオレンジ・ブックにより定められる他の特殊または付加的な情報は、ディスク製造者に既知の特殊な値に設定されることが可能である。これらの値は単独で又は組み合わせて、予め形成されたＩＤ２２コードを算出するために使用可能である。

【００２４】ディスク１０は第２セッション１６を含み、ＣＤ－ＷＯまたはＣＤ－ＲＷライタのような再記録可能な光学ディスク技術を利用して書き込まれたものである。ディスク１０は、第３セッションを含むことも可能であり、あるいは更に後続の書き込み済みセッション(written session)を含むことも可能である。ディスク１０は、ユーザの再記録可能な領域２０をも包含する。記録済みのセッションに含まれているものは、固有の識別番号またはＩＤ２４および暗号化された実行可能な(executable)パッケージ３０であり、ＩＤ２４は１つ又はそれ以上の既知の絶対セクタ・アドレスにおける第２セッションに書き込まれる。

【００２５】図２を参照するに、本発明で使用する実行可能なプログラムを暗号化する手法の１つが示されている。実行可能なパッケージはディスク１０に書き込まれる。暗号化されたパッケージは６つの実行可能なプログラム３０を含み、これはディスク１０において当初の実行可能なプログラム４０と同一名称を有する。パッケージ３０は、最初に走るラッピング(wrapping)ソフトウエアを含む。このパッケージは、プログラムが走っている際に、ハッキング・ソフトウエアの存在を検査するサブルーチン３４も含む。また、データ、命令または両者より成る多形態セクション３６も存在する。概して多形態コードは、同一結果に導く複数の経路を提供するが、プログラムが実行される各々の場合に異なる経路をたどるように構成される。多形態コードは、そのプログラムに対するリバース・エンジニアリングを一層困難にするために使用される。暗号解除ルーチン３８は、プログラム可能なＣＤ－ＲＯＭに格納されたデータ（特に、予め形成されたＩＤ２２および固有のＩＤ２４）を利用するために指定され、実行可能なもの４０の暗号化を解除する。

【００２６】図３を参照するに、ユーザの実行可能なプログラムを暗号化するのに必要なステップが示され、それを暗号化するためにプログラム可能なＣＤ－ＲＯＭの特性を利用する。これは、本願で詳細に説明される様々な本願実施例で使用可能である。ステップ４８において、プログラム可能なＣＤ－ＲＯＭ上に又は局所的なハード・ドライブ上もしくは配信ネットワーク上にマスタされた(mastered)暗号化プログラム可能なＣＤ－ＲＯＭが、コンピュータのメモリ内に読み込まれる。ステップ５０において、暗号化を要する実行可能なファイルがメモリに読み込まれる。ステップ５２において、ソフトウエア・アプリケーションを拡布する者またはプログラム可能なＣＤ－ＲＯＭを利用する存在として定められる顧客は、マスタされたプログラム可能なＣＤ－ＲＯＭディスクをＣＤ－ＲＯＭライタに置く。

【００２７】顧客が暗号化されるべきファイルを指定することによって開始する。これらのファイルは、データおよび実行可能なプログラムの両者または実行可能なプログラムだけを含み得る。その後顧客は、暗号化されたソフトウエアが書き込まれるべきプログラム可能なＣＤ－ＲＯＭディスクに関する予め形成されたＩＤ２２および固有のＩＤ２４に対応する情報を入力する。他の実施例にあっては、これらの値は、それらが記録される任意の場所からプログラム可能なＣＤ－ＲＯＭから読み出される。セキュリティ・ソフトウエアが予め形成されたＩＤ２２および固有のＩＤ２４を取得すると、ステップ６２において、それらを共に利用して暗号キーを作成する。暗号化プログラム６３は、ステップ６４においてその暗号キーを利用し、実行可能なファイルおよびセキュリティ・レベル・テーブルを暗号化する。ステップ６４で暗号化されたファイルは、その後ステップ７０においてラッパ(wrapper)プログラムにデータ ファイルとして付加される。ラッパ・プログラムは、セキュリティ・テーブルにおける指定によって許容されるようなディスク１０からの予め形成されたＩＤ２２および固有のＩＤ２４を読み込むのに必要なサブルーチンと、プログラムが走っているコンピュータのメモリ内にリバース・エンジニアリング・ツールが存在することを検出し、それらが検出された場合には実行を中断させるサブルーチンと、ソフトウエア・アプリケーションの暗号化解除および実行を開始するサブルーチンとを含む。ステップ７２において、ラップされた実行可能パッケージは、書き込み可能セッション（１６または１８）においてプログラム可能なＣＤ－ＲＯＭディスクに書き込まれる。

【００２８】暗号作成法および暗号化機能は当該技術分野で周知である。これに関し、Applied Cryptography, B.Schneier, John Wiley and Sons, Inc., New York, 1996に適切な記載があり、この内容は本願でも使用可能である。本実施例では、以下の表記方法を採用する：

表１

暗号化標記

記号	意味
Ｐ	暗号化されるべきプログラム
Ｅ	暗号化関数
Ｂ	予め形成されたＩＤ
Ｕ	固有のＩＤ
Ｉ	連結したＩＤ＝ＢＵ
Ｘ	暗号化されたプログラム＝Ｅ（Ｐ，Ｉ）

本発明に関し、以下の条件を満足する任意の暗号化関数が利用可能であり、それは：Ｅ（Ｐ，Ｉ）の計算が実行可能に適切であること，すなわちＥが多項式タイム(polynomial time)で計算可能であること；E^{-1}（Ｘ，Ｉ）

の計算に関する多項式タイム・アルゴリズムが既知であって実行可能に適切であること；暗号化関数E（およびその解読に相当するE^{-1}）が、その計算の際に提供される可変なキーＩを利用すること；および暗号化／暗号解除プロセスを通じて良好でないプログラムP'（P'=E^{-1}{E(P,I),I}）を形成してしまう蓋然性が非常に小さいこと、である。

【００２９】暗号化のステップは以下のとおりである：

１．予め形成されたＩＤ　Ｂおよび固有のＩＤ　Ｕを取得する；

２．２つのＩＤが連結され（Ｉ＝ＢＵ）、暗号化／暗号化解除キーＩを求める；

３．暗号化アルゴリズムＥで連結されたＩＤが使用され、暗号化されたプログラムＸ＝Ｅ（Ｐ，Ｉ）を計算する；

暗号化解除のステップは以下のとおりである：

１．予め形成されたＩＤ　Ｂおよび固有のＩＤ　Ｂを取得する；

２．２つのＩＤが連結され（Ｉ＝ＢＵ）、暗号化／暗号化解除キーＩを求める；

３．暗号化解除アルゴリズム$Ｅ^{-1}$で連結されたＩＤが使用され、当初のプログラム$Ｐ＝Ｅ^{-1}$（Ｘ，Ｉ）を計算する；

図４を参照するに、本発明の第１実施例に関するブロック図が示される。マスタ・コンパクト・ディスクに関する周知のマスタ技術を利用して、プログラム可能なＣＤ－ＲＯＭディスクがマスタされる（ステップ８０）。この点に関し、例えば上述の共通して譲渡される米国特許出願番号09／662,561がある。プログラム可能なＣＤ－ＲＯＭは第１セッション１４を含むが、それに加えて他のマスタ・セッションを含むことも可能である。マスタ・ディスクに含まれるものは、予め形成されたＩＤ２２である。その後ステップ８２において、マスタ・ディスクを利用して、標準的なスタンプ(stamp)手法によりプログラム可能なＣＤ－ＲＯＭディスクを製造する。この時点では、多数の同一のプログラム可能なＣＤ－ＲＯＭディスクが存在する。

【００３０】その後ディスク１０は各自の識別子を利用して書き込まれる。ステップ８４において、固有のＩＤ２４が形成される。固有のＩＤ２４は、ディスク１０の製造順によって定められるところの連続的に定められた番号とすることが可能であり、完全にランダムな番号とすることも可能であり、または予め形成された番号のテーブルから選択することも可能である。他の好適な実施例では、その番号はアルゴリズムによって更に処理され、そのアルゴリズムは、有効な番号(valid number)はとり得る番号の範囲内の小さな部分にのみ対応しているように使用番号(actual number)を生成可能である。この場合、有効な番号は、そのような生成アルゴリズムを知ることによってのみ作成可能である。また、この場合は、検査アルゴリズムを提供し、例えば周知の公開キー，プライベート・キー暗号化および署名の手法を利用することによって、番号を認めることも可能である。他の実施例では、その番号はハードウエア身元確認により生成され、特定のコンピュータに関連付けられる。（この点については、例えばO' Connor et al., U.S. 5,745,568があり、本願でも使用可能である。）他の実施例では、固有のＩＤ２４が特定のアプリケーションに関連付けられ、このため同一の固有の識別番号が複数のディスク１０上で使用される。固有のＩＤ２４は、書き込み済みセッションとなるＩＳＯ９６６０両立可能ファイル・イメージを作成するために使用される（ステップ８６）。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のＩＤ２４を利用して修正され（ステップ８８）、ステップ９０において第２セッション１６としてディスク１０に加圧されずに書き込まれる。なお、このセッションは第３またはそれ以降のセッションとして書き込まれることも可能である。この時点において、各ディスク１０は、各自自身の識別子を包含し、特有のものとなる。

【００３１】顧客は暗号化に備えてディスク１０を用意する。この段階は、ステップ７４として図示され、図３で詳細に説明したセキュリティ・ソフトウエアによって実行される複数のステップより成る。固有のＩＤ２４は、第２セッション１６における既知の絶対セクタ・アドレスから読み取られる（ステップ９２）。暗号化は、ステップ７６として図示され、図３で詳細に説明した多数のステップより成る。暗号化が完了すると、ディスク１０上の第３セッション１８にラップされた実行可能なものが書き込まれる（ステップ９４）。

【００３２】図５を参照するに、本発明の第２実施例のブロック図が示され、固有のＩＤ２４および暗号化された実行可能なもの４０が同じセッションに書き込まれている。これは、図４で説明したものと同じステップをいくつか含んでいるが、その順序が異なる。プログラム可能なＣＤ－ＲＯＭディスクは、マスタ・コンパクト・ディスクに関して周知のマスタ技術を利用してマスタされる（ステップ８０）。この点に関し、例えば上述の共通して譲渡される米国特許出願番号09／662,561がある。プログラム可能なＣＤ－ＲＯＭは第１セッション１４を含むが、さらに他のマスタ・セッションを含むことも可能である。ディスク１０に含まれているものは予め形成されたＩＤ２２である。その後ステップ８２において、マスタ・ディスクを利用して、標準的なスタンプ手法によりプログラム可能なＣＤ－ＲＯＭディスクを製造する。この時点では、多数の同一のプログラム可能なＣＤ－ＲＯＭディスクが存在する。

【００３３】顧客は暗号化に備えてディスク１０を用意する。この段階は、ステップ７４として図示され、図３で詳細に説明したセキュリティ・ソフトウエアによって

実行される複数のステップより成る。固有のＩＤ２４がステップ８４で形成される。固有のＩＤ２４は完全にランダムな番号とすることが可能であり、予め形成された番号のテーブルから選択することも可能である。固有のＩＤ２４は、書き込み済みセッションとなるＩＳＯ９６６０両立可能ファイル・イメージを作成するために使用される（ステップ８６）。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のＩＤ２４を利用して修正される（ステップ８８）。ステップ７４で読み込んだ予め形成されたＩＤ２２と共に、固有のＩＤ２４を利用して、暗号化を行う。暗号化は、ステップ７６として図示され、図３で詳細に説明した多数のステップより成る。暗号化が完了すると、ディスク１０上の第３セッション１８にラップされた実行可能なものが書き込まれる。

【００３４】図６を参照するに、本発明によるエンド・ユーザで実行するための方法が示される。まず、エンド・ユーザはディスク１０をＣＤ－ＲＯＭ，ＣＤ－ＲまたはＣＤ－ＲＷドライブにディスク１０を挿入する（ステップ１００）。ディスク１０上で実行可能なプログラムが自動的に走り出しまたは選択される（ステップ１０２）。プログラムは先ず対ハッキング(anti-hacking)サブルーチン３４を使用して、ハッキングまたはコピー・プロテクト対策を打ち破るために使用され得るカーネル・デバッグ・ソフトウエア(kernel-debugging software)の検査を行う（ステップ１０４）。そのようなプログラムが存在すると、そのプログラムはユーザにエラー・メッセージを示し、自動的に停止する（ステップ１０６）。

【００３５】そのようなハッキング・ソフトウエアがエンド・ユーザのシステムに存在しない場合は、ステップ１０８において暗号化解除プログラムがドライブＩＤを読み出す。ステップ１１０において、暗号化解除プログラムは、そのドライブに対して、ＡＴＩＰ信号から予め形成されたＩＤ２２を読み出すための命令を発行する。そして、ステップ１１６において、暗号化解除プログラムは、そのドライブに対して、第２の（後続の）セッションの主データ・チャネルの既知の絶対セクタ・アドレスから固有のＩＤ２４を読み出すための命令を発行する。

【００３６】ステップ１１８において、暗号化解除プログラムは、ステップ１１６で読み込んだ固有のＩＤ２４と、ステップ１１０でＡＴＩＰから読み込んだ予め形成されたＩＤ２２とを連結する。ステップ１２０において、その連結された結果を暗号化解除キーとして利用して、ラップされたソフトウエア３２の暗号化を解除する。ステップ１２２において、プログラムは、その暗号化解除が有効であるか否かを判定する。これを行ういくつかの手法が存在し、例えば、暗号化解除されたプログラム内のフラグを探索したり、オペレーティング・システム固有のコードが暗号化解除された実行可能なものの中に存在するか否かを検査することが可能である。暗号化解除に失敗すると、エラー・メッセージが示され、そのプログラムーおよび全プロセスーが終了する（ステップ１０６）。暗号化解除が成功すると、当初の実行可能なものが開始される（ステップ１２４）。

【００３７】暗号化解除プログラムは背景に残り（ステップ１４８）、プログラムは実行され（ステップ１４６）および抜け出す（ステップ１５０）。当初のプログラムが抜け出ると、暗号化解除プログラムは、メモリおよび当初プログラムの使用したハード・ドライブの領域をクリアし（ステップ１５２）、終了する（ステップ１５４）。

【００３８】図７を参照するに、本発明が様々な不当な試みからどのようにして保護するかが示されている。例えば、不正な者が正当なプログラム可能なＣＤ－ＲＯＭディスクのコピーを作成し、それには、使用許諾されてはいるが各自から更に拡布することは認められていないソフトウエアを含んでいる場合がある。目下利用可能なディスク・ライタを利用しておよびソフトウエアを書き込んで、ＣＤ－Ｒディスクにコピーを行うことが可能である（ステップ１６０）。しかしながら、予め形成されたＩＤ１１がディスク１０のＡＴＩＰに含まれており、これはコピーされ得ない。ＣＤ－Ｒディスク不正者は、ＡＴＩＰ信号に暗号化された予め形成されたＩＤ２２を既に所有している、または予め形成されたＩＤ２２を何ら所有していない。このような場合において、偽造のディスクによる実行可能なプログラム３０の実行は、正しくない予め形成されたＩＤを形成し（ステップ１６２）、暗号化解除に失敗してしまう（ステップ１６４）。

【００３９】また、不正者が1つ又はそれ以上の正当に登録されたプログラムを有するプログラム可能なＣＤ－ＲＯＭディスクを有するが、他のユーザのプログラム可能なＣＤ－ＲＯＭディスクから他のプログラムを不当にコピーする場合がある（ステップ１６６）。この分配が同一の分配者によるものである場合、ソースおよびターゲット・ディスクは同一の予め形成されたＩＤ２２を有する。しかしながら、盗まれたプログラムは、それが配信元(originator)により正当に登録されているならば、予め形成されたＩＤ２２および配信元の固有のＩＤの組み合わせによって暗号化される。不正者が盗んだプログラムを走らせようとする場合に、プログラムは、予め形成されたＩＤと不正者の固有のＩＤ（配信元の固有のＩＤとは異なる）とを利用して暗号化解除が行われる（ステップ１６８）。この手順は正しくないキーを形成し、ステップ１６４で暗号化に失敗する。

【００４０】配信元から上記のプログラムを不当にコピーする際に、不正者が固有のＩＤ２４の重要性に気付いており、そのコピーをも形成する場合がある（ステップ

１７０）。固有のＩＤ２４は、ユーザの書き込み可能な領域内におけるディスク１０の新たな部分に書き込まれる（ステップ１７２）。しかしながら、暗号化解除プログラム３０は、ステップ１１６において、その固有のＩＤ２４が所定の場所にあることを期待している。したがって、暗号化解除プログラムは、ステップ１６８において不当な固有ＩＤを利用して、配信元の固有のＩＤを利用して暗号化されているプログラムの暗号解除を試み、その暗号化解除に失敗する（ステップ１６４）。

【００４１】不正者が固有のＩＤ２４だけでなく、所定の場所に位置する必要性にも気付いている場合もあり得る。その者は、ステップ１７０においてソフトウエアおよび固有のＩＤ２４をコピーする際に、配信元の固有のＩＤが、ディスク１０上に既に位置している固有のＩＤ２４に上書きされるように、巧妙な制御を行うこともあり得る（ステップ１７４）。しかしながら、ディスク１０への１文字の書き込みであっても、古い固有のＩＤ２４が消去されることは許容されず、利用できない新たな固有のＩＤを書き込んでしまう（ステップ１７６）。ディスク１０におけるプログラムの更なる暗号化解除は失敗してしまう（ステップ１６４）。

【図面の簡単な説明】

【図１】図１は、本発明によるコピー・プロテクトを有するコンパクト・ディスクの平面図である。

【図２】図２は、コピー不可能にアプリケーションを暗号化するソフトウエア手法の概略図である。

【図３】図３は、暗号化されたソフトウエアを形成するためのステップを示すブロック図である。

【図４】図４は、コピー・プロテクトがＣＤにどのように提供されるかの一例を示すブロック図である。

【図５】図５は、コピー・プロテクトがＣＤにどのように提供されるかの他の例を示すブロック図である。

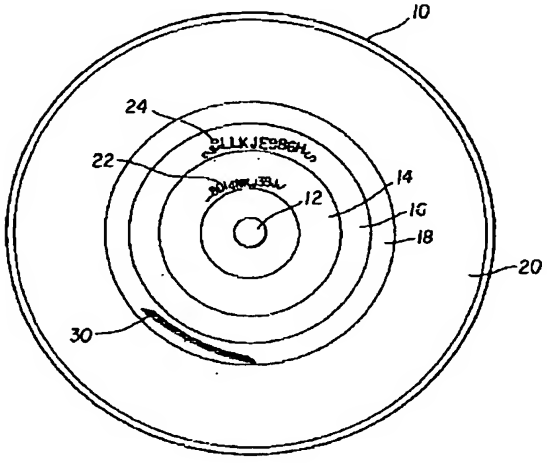
【図６】図６は、ＣＤが読み込まれる場合に、コピー・プロテクトがどのように機能するかを示すブロック図である。

【図７】図７は、ここに開示したコピー・プロテクトが、それを破ろうとする方法をどのようにして阻止するかを示すブロック図である。

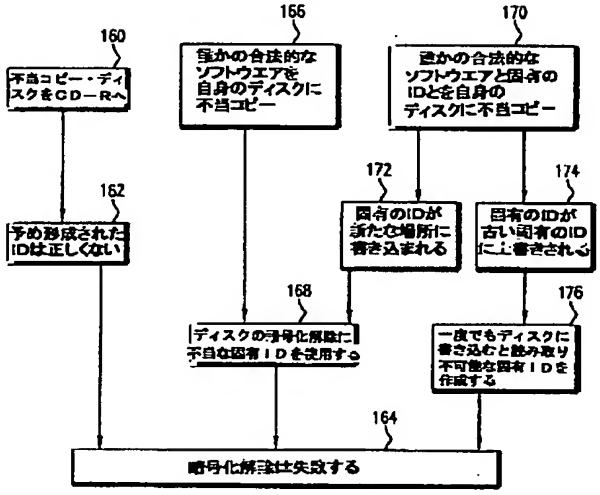
【符号の説明】

１０　光学ディスク
１４　第１セッション
１６　第２セッション
１８　第３セッション
２０　再記録可能な領域
２２　予め形成されたＩＤ
２４　固有のＩＤ
３０　パッケージ

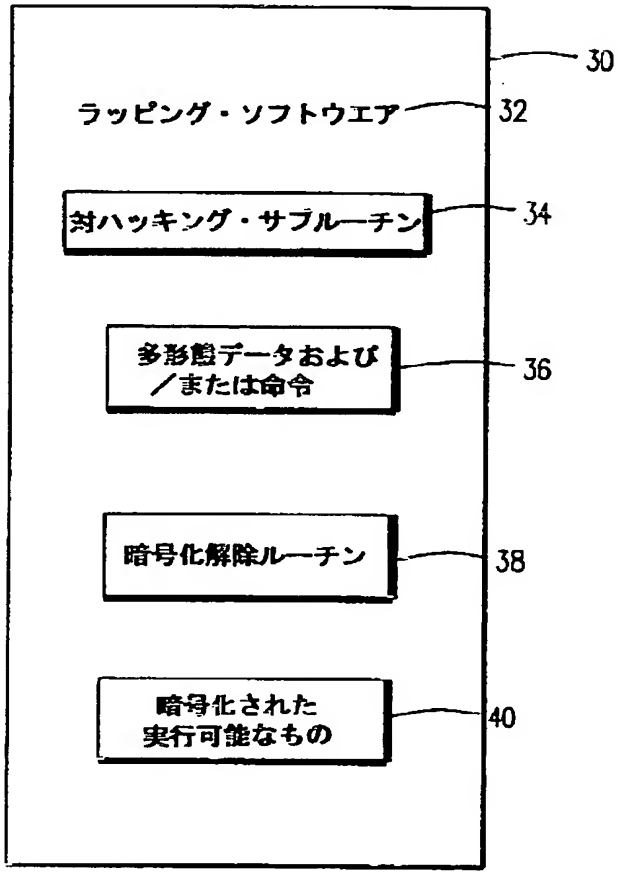
【図１】



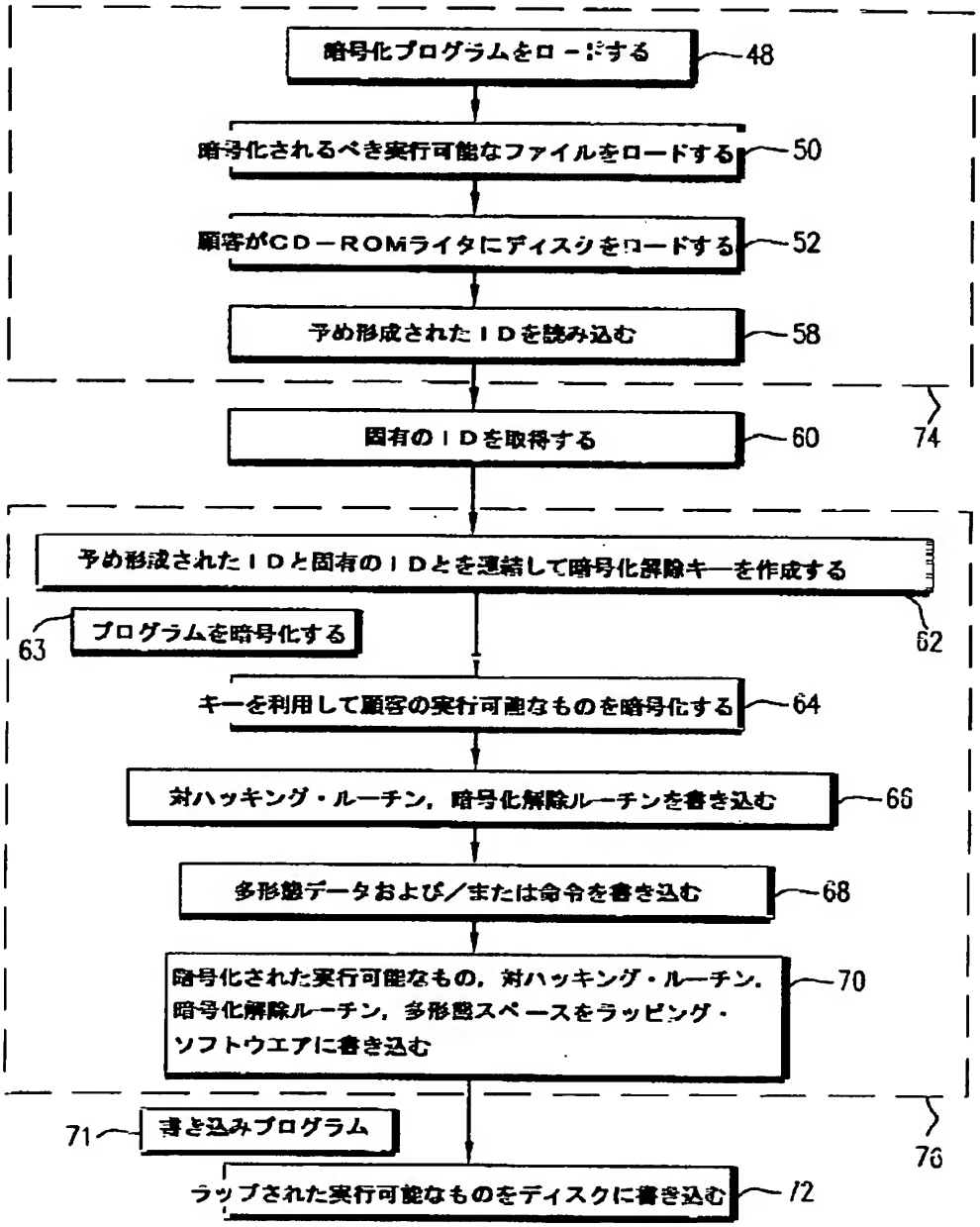
【図７】



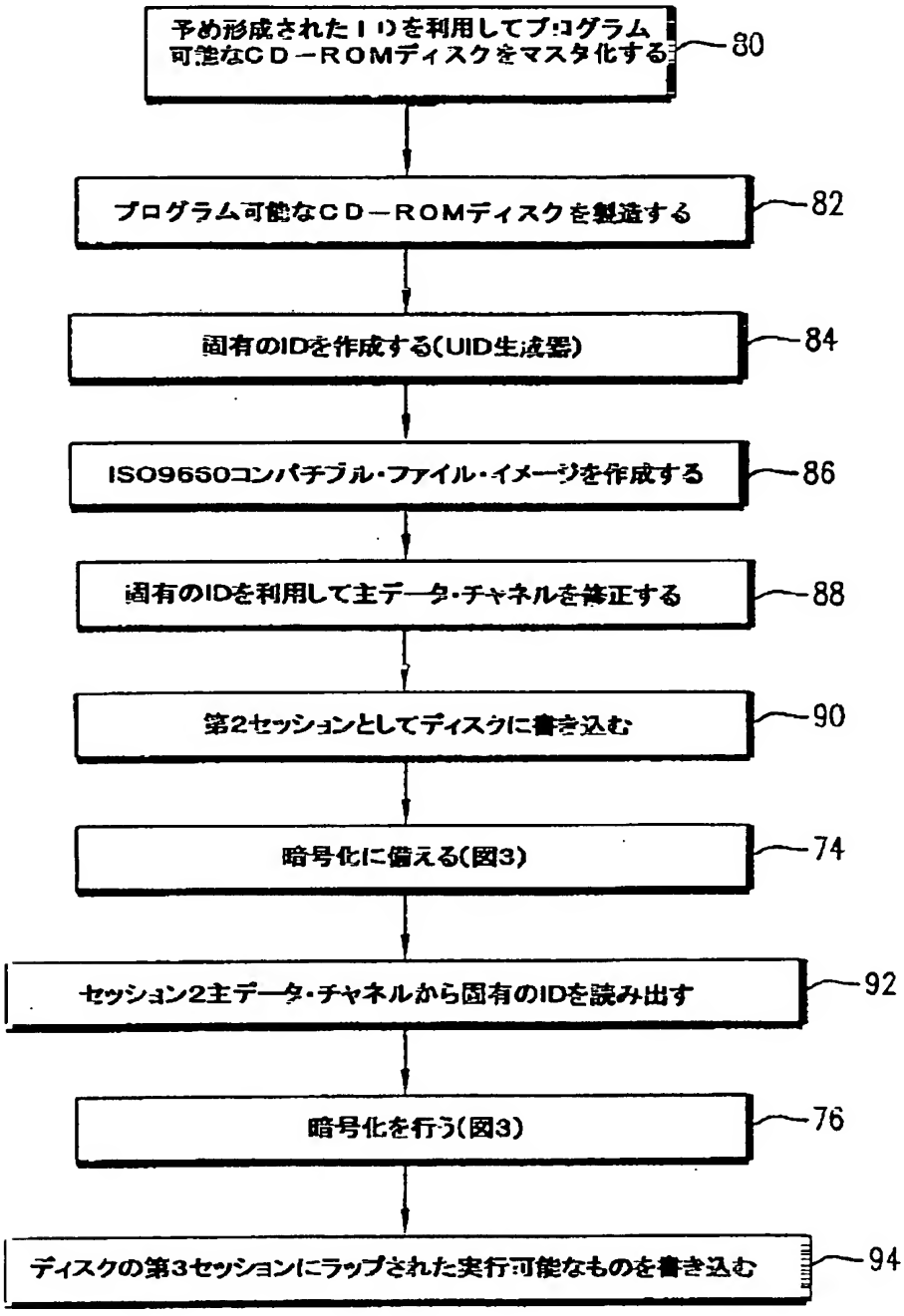
【図2】


30
ラッピング・ソフトウエア
32
対ハッキング・サブルーチン
34
多形態データおよび
／または命令
36
暗号化解除ルーチン
38
暗号化された
実行可能なもの
40

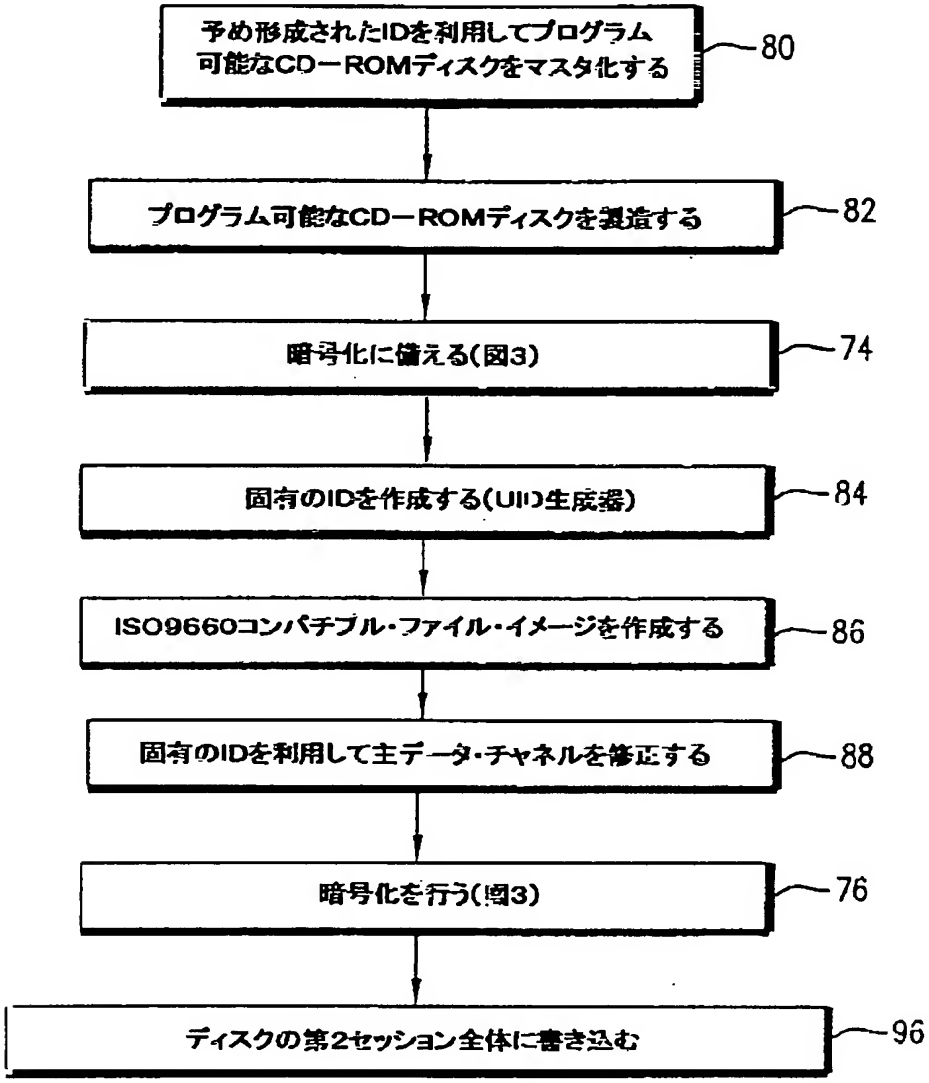
【図3】


暗号化プログラムをロードする
48
暗号化されるべき実行可能なファイルをロードする
50
顧客がCD-ROMライタにディスクをロードする
52
予め形成されたIDを読み込む
58
74
固有のIDを取得する
60
予め形成されたIDと固有のIDとを連結して暗号化解除キーを作成する
62
63
プログラムを暗号化する
キーを利用して顧客の実行可能なものを暗号化する
64
対ハッキング・ルーチン，暗号化解除ルーチンを書き込む
66
多形態データおよび/または命令を書き込む
68
暗号化された実行可能なもの，対ハッキング・ルーチン，暗号化解除ルーチン，多形態スペースをラッピング・ソフトウエアに書き込む
70
76
71
書き込みプログラム
ラップされた実行可能なものをディスクに書き込む
72

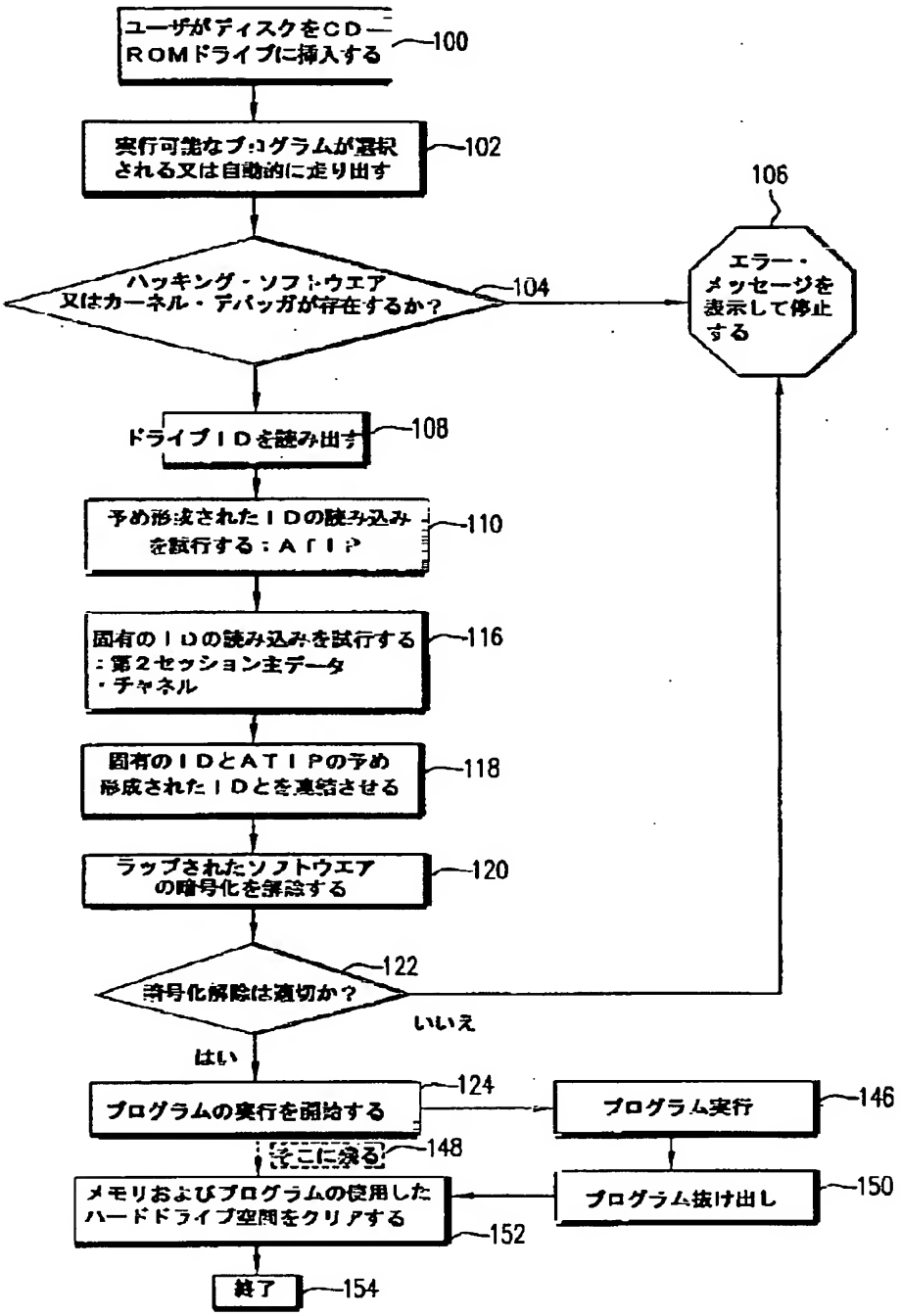
【図4】


予め形成されたIDを利用してプログラム可能なCD−ROMディスクをマスタ化する
80
プログラム可能なCD−ROMディスクを製造する
82
固有のIDを作成する(UID生成器)
84
ISO9660コンパチブル・ファイル・イメージを作成する
86
固有のIDを利用して主データ・チャネルを修正する
88
第2セッションとしてディスクに書き込む
90
暗号化に備える(図3)
74
セッション2主データ・チャネルから固有のIDを読み出す
92
暗号化を行う(図3)
76
ディスクの第3セッションにラップされた実行可能なものを書き込む
94

【図５】


予め形成されたIDを利用してプログラム可能なCD-ROMディスクをマスタ化する
80
プログラム可能なCD-ROMディスクを製造する
82
暗号化に備える(図3)
74
固有のIDを作成する(UID生成器)
84
ISO9660コンパチブル・ファイル・イメージを作成する
86
固有のIDを利用して主データ・チャネルを修正する
88
暗号化を行う(図3)
76
ディスクの第2セッション全体に書き込む
96

【図6】



フロントページの続き

(51)Int.Cl.⁷	識別記号	ＦＩ	(参考)
Ｇ１１Ｂ 20/12		Ｇ１１Ｂ 20/12	

(72)発明者 ブルース エル ハ
アメリカ合衆国 ニューヨーク 14580
ウェブスター レイク・ロード 1072

Fターム(参考) 5B017 AA06 AA07 BA07 CA09 CA15
5D044 BC03 CC04 DE49 GK17
5D090 AA01 BB02 CC12 FF09 GG32
HH01
5D121 JJ05 JJ08 JJ09